REMARKS

Applicant notes that the amendment proposed for claim 13 in the prior Reply was not entered, apparently because the status was incorrectly indicated as "original" rather than "currently amended." Applicant in this response has presented the amendment to claim 13 with the correct status and asks that it be entered.

Applicant has also made minor amendments to certain of the claims to recite "connection table" when the claim merely referred to "table" for clarity. Applicant has also amended claims 1 and 8 to call for a computer implemented method and that the connection table is stored in a computer readable medium, e.g., memory, storage and so forth.

Allowable Subject Matter

The examiner indicated that Claims 5, 13 and 18 were objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Applicant thanks the examiner for the indication of allowable subject matter. However Applicant believes that all of the claims are allowable for reasons discussed below.

35 U.S.C § 102

The examiner rejected Claims 1-4, 6-17 and 19-36 are rejected under 35 U.S.C. 102(e) as being anticipated by Pruthi (20040015582). The examiner argues that:

> **As per claim 1, Pruthi discloses: adding host-pair connection records to a connection table when a host accesses another host (0036, 0039, 0187); at the end of a first update period, accessing the connection table to determine new host pairs (0039);**
>
> **determining the number of new host pairs added to the table over the first update period (0187); and if a host has made more than a first threshold number "C 1" host pairs, a historical number of host pairs in the profile is smaller than the threshold number by a first factor value "C2", then indicating to a console that the new host is a scanner (0187, 0204-0205).**

Claim 1, as presented is allowable over Pruthi at least because Pruthi neither describes nor suggests "... adding host-pair connection records to a connection table when a host accesses

another host ... accessing the connection table ... determining the number of new host pairs added to the table over the first update period; and if a host has made more than ... "C1" host pairs, and an historical number of host pairs is smaller than the threshold number by a first factor value "C2", then indicating that the new host is a scanner.

Pruthi neither at "**(0036, 0039, 0187)**" nor elsewhere suggests, much less describes the feature of "adding host-pair connection records to a connection table." Pruthi discusses collection of network statistics but does not determine "host pair connections." Therefore, Pruthi inherently cannot describe or possess the feature of "**accessing the connection table to determine new host pairs (0039).**" For instance in [0039] relied on by the examiner to show the feature of accessing the connection table to determine new host pairs, Pruthi merely discloses "programming to generate statistics." No mention is made of tracking of network connections among hosts, much less the claimed feature.

The examiner also relies on Pruthi to describe **determining the number of new host pairs added to the table over the first update period (0187).**" However, as pointed out above Pruthi neither describes nor suggests "host pairs" whether at [0187] or elsewhere.

Pruthi does mention scans. However, Pruthi does not detect scans in the manner called for by claim 1. The examiner relies on [0187, 0202-0205] for the features of Applicant's claim pertaining to indicating that a new host is a scanner. Pruthi describes in the relied on passages:

> **[0187] For a particular set of applications, the number of IP host pair connections involving a common IP address (either the source or destination) exceeds x over a time window of y. x and y should be user configurable. The set of applications should include a set of positive rules, e.g. telnets and pings, as well as negative rules such as "not http". This can be used to track Denial of Service attacks and IP host scans.**
>
> **[0204] Ability to determine when network activity is exceeding "normal thresholds" (bandwidth spikes for extended periods)**
>
> **[0205] Ability to specify the time span and height of the spike which would be considered excessive**

At the outset, Applicant notes that the examiner rejected claim 1, as being anticipated by Pruthi. That feature of claim 1, pertaining to determining scanners requires: determining the number of new host pairs added to the table over the first update period. Applicant contends that not only does Pruthi fail to disclose the table; Pruthi fails to determine the number of new host pairs added to the table over a first period. Pruthi merely determines "**the number of IP host pair**

connections involving a common IP address (either the source or destination) exceeds x over a time window of y." This however is neither relevant to nor determines new host pairs.

The claimed feature also requires evaluation of two thresholds i.e., "if a host has made more than ... "C1" host pairs," and requires determining if ... the number C1 is smaller than "an historical number of host pairs" by a first factor value "C2" to indicate that the new host is a scanner. Pruthi has two user configurable variables "**the number of IP host pair connections involving a common IP address**" that exceeds "**x**" and "**y**" a "**time window.**" While Applicant does not concede that "**x**" corresponds to "C1," it is quite clear that Applicant requires three items, "C1," an update period and "C2."

Accordingly at least for these reasons Pruthi neither describes nor suggests claim 1.

Claim 8

Claim 8 is neither described nor suggested by Pruthi. Claim 8 includes the features of "... retrieving from a connection table logged values of protocols and ports used in host pair connections records ... determining if the number of ports used in an historical profile is smaller by a factor "C1" than a current number of ports being scanned by a host and if the current number is greater than ... "C2" recording an anomaly and reporting a port scan."

The examiner argues:

> **As per claim 8, 20 and 33, Pruthi discloses: retrieving from a connection table logged values of protocols and ports used in host pair connections records in the table (0046);**
>
> **determining if the number of ports used in the historical profile is considerably smaller by a factor "C1" than a current number of ports being scanned by a host and the current number is greater than a lower-bound threshold "C2", to record the anomaly (0187, 0204-0205); and reporting a port scan to a console (0187, 0204-0205).**

Pruthi describes in the relied on passage [0046]:

> **[0046] An incoming bitstream is packetized by a packetizer 502. Decoding of the bitstream may be automatically performed for known protocols or may be performed according to user-specified parameters for custom or proprietary protocols. For example, if a new data link layer protocol is introduced, network monitor 500 includes suitable programming to respond to user-defined protocols, entered using the user interface 520. The inventive network monitor 500 thus recognizes packet structures of the new protocol to packetize an incoming bitstream. The network monitor could then perform its data collection and analysis methods**

through the higher protocol layers. This flexibility is not limited to the data link layer. In other words, the network monitor 500 according to the present invention is able to collect and analyze data communications for custom protocols at other protocol layers.

Nothing in the cited passage of Pruthi describes any feature that is equivalent to the claimed connection table. In this passage, Pruthi describes decoding of a bitstream according to custom or proprietary protocols. However, that is not relevant to the claimed feature of "retrieving from a connection table logged values of protocols and ports used in host pair connections records ..." Pruthi clearly discusses protocols and ports, but in Pruthi these data are not associated with host pair connection records, as claimed in claim 8.

Claim 8 also includes the feature of: "determining if the number of ports used in an historical profile is smaller by a factor "C1" than a current number of ports being scanned by a host and if the current number is greater than ... "C2 recording an anomaly and reporting a port scan" While the examiner is free to apply reasonable interpretations to claims, Applicant contends that the examiner's use of Pruthi [0187] for this feature contradicts the examiner's use of Pruthi for the feature of claim 1.

Moreover, Pruthi as applied to claim 8 suffers from an analogous deficiency as it does when applied to claim 1. Pruthi has two user configurable variables "**the number of IP host pair connections involving a common IP address**" that exceeds "**x**" and "**y**" a "**time window.**" Claim 8 by contrast has a factor "C1" and threshold "C2."

Claims 14, 24 and 28

Claims 14, 24 and 28 includes the features of (or analogous features): "instructions ... to add host-pair connection records to a connection table when a host accesses another host ... determine new host pairs ... added to the table over the first update period and if a host has made more than a first threshold number "C1" host pairs, and an historical number of host pairs is smaller than the threshold number by a first factor value "C2", then indicate to a console that the new host is a scanner.

Pruthi neither at "**(0036, 0039, 0187)**" nor elsewhere suggests, much less describes these features for analogous reasons as discussed for claim 1.

Claims 2, 15, 25 and 29

Claims 2, 15, 25 and 29, are allowable at least for the reasons discussed in claims 1, 14, 24 and 28. Pruthi does not disclose two adjustable thresholds e.g., "Cl" and "C2," but merely a factor "x" and a time window "y," whether at [0187-0188] or elsewhere.

Claims 3, 16, 26 and 30

Claims 3, 16, 26 and 30 are allowable over Pruthi because Pruthi neither describes nor suggests "the connection table," as argued above and therefore does not suggest the added feature of "a current time-slice connection table ... ."

Claims 4, 17, 27 and 31

Claims 4, 17, 27 and 31 are allowable over Pruthi because Pruthi neither describes nor suggests "aggregating records from the current time-slice table into a long update period table, the second update period table having a period that is greater in duration than the first update period," whether at [0041] or elsewhere.

The examiner argues that Pruthi describes: "**checking for ping scans at the end of a long update period (Column 7, Lines 30-45).**" **Column 7, Lines 30-45** are not findable in Pruthi. Clarification is requested.

Nonetheless, Pruthi neither describes nor suggests: "indicating hosts which produced more than "C3" new host pairs over the second update period," whether at [0187-0190] or elsewhere. Again this analysis suffers from the same deficiencies as pointed out above. The examiner uses the same teachings against these features, which are additional features applied to the base claims. Moreover, these claims call for an additional threshold, which Pruthi clearly does not possess.

Claims 6 and 19

Claims 6 and 19 are allowable over Pruthi because while Pruthi discloses ARP packets, which assuming are "Address Resolution Protocol" packets, Pruthi does not disclose the claimed "connection table" and the feature that "for sparse subnets tracking the number of generated ARP

requests that do not receive responses to detect scans on sparse sub-networks," whether at [0035, 0042, 0109, 0202] or elsewhere.

Claims 9, 21 and 34, and claims 10, 22 and 35

Claims 9, 21 and 34, and claims 10, 22 and 35 serve to further distinguish claims 8, 20 and 33 at least because Pruthi fails to describe "a severity level," as applied to port scans.

Claims 11, 23 and 37

Claims 11, 23 and 37 serve to further distinguish claims 8, 20 and 33over Pruthi at least because Pruthi fails to disclose: "the connection table" or using statistics regarding TCP reset (RST) packets and ICMP port-unreachable packets ... relative to the profile to increase the severity of a port scan event, whether at [0035, 0114, 0165, 0219] or elsewhere.

Claim 12

Claim 12 is allowable at least for the reasons discussed in claim 8.

Please charge the Petition for Extension of Time fee of **$60** to Deposit Account No. 06-1050. Please apply any other charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: July 17, 2008

/Denis G. Maloney/
Denis G. Maloney
Reg. No. 29,670

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110
Telephone: (617) 542-5070
Facsimile: (877) 769-7945